Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Ministerie van Veiligheid en Justitie
t.a.v. directeur van de directie Informatisering en Inkoop

Turfmarkt 147
2511 DP Den Haag

Auditdienst Rijk

Turfmarkt 147
2511 DP Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

Ons kenmerk
ADR/ 2015/963

Bijlagen

Datum: 1 juli 2015
Betreft: Overzicht bevindingen ADR Governance en financieringsmodel.

Doel van het onderzoek
De projectorganisatie van de 'Gezamenlijke aanpak Biometrie' heeft de ADR gevraagd kritisch mee te lezen bij de door de projectorganisatie opgestelde beschrijving van de governance, inclusief het daarbij behorende financieringsmodel. Het doel van ons onderzoek was om de projectorganisatie te wijzen op mogelijk ontbrekende of onvolledige onderwerpen in de hiervoor genoemde beschrijving. De onderzoeksvraag hebben wij als volgt geformuleerd:
Welke verbeterpunten signaleren wij in de beschrijving van de governance en het bijbehorende financieringsmodel?
In deze notitie beschrijven wij onze bevindingen, waarbij antwoord wordt gegeven op bovenstaande onderzoeksvraag.

Scope en diepgang
Ons onderzoek heeft zich, conform plan van aanpak, beperkt tot het bestuderen van de beschrijvingen over:
- de governance (sturen, beheersen, verantwoorden en toezichthouden) op strategisch, tactisch en operationeel-niveau van het ABIS-systeem en
- de verdeling van de kosten na het in bedrijf nemen van het ABIS-systeem (service).

Deze beschrijvingen zijn opgenomen in het document "Advies Governance- en Financieringsmodel. Gezamenlijke aanpak Biometrie. Versie 1.0, concept, d.d. 15 juni 2015."
Waar nodig is om aanvullende informatie gevraagd. Voor de context hebben wij kennisgenomen van: de Business Case voor het project (versie 1.0, definitief, d.d. 17 december), de Architectuur Visie (versie 1.0, definitief, d.d. 4 december 2014), de projectbrief (versie 1.0, definitie, d.d. 15 mei 2014) en de Project Start Architectuur (PSA) (versie 9 april 2015). Deze documenten vallen buiten de scope van ons onderzoek. Desondanks hebben wij gemeend enkele aandachtspunten te formuleren voor de business case en de PSA.
Het onderzoek is uitgevoerd volgens de NBA- richtlijn 4400 "Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot

financiële informatie". Dit betekent dat geen assurance wordt verstrekt en geen oordeel wordt gegeven, maar dat bevindingen worden benoemd.
Deze notitie is in concept op 30 juni 2015 besproken met de gedelegeerd opdrachtgever ' (projectmanager Biometrie).

Bevindingen Governance en financieringsmodel

Het document geeft een eerste aanzet voor de governance rondom de biometrie-oplossing. Zoals omschreven in het document zelf dienen veel essentiële punten nog nader te worden uitgewerkt. Het toetsen aan een norm is daarom nog weinig zinvol. Daarom volstaan wij met het weergeven van een aantal noties en aandachtspunten.
Hieronder wordt eerst ingegaan op bevindingen met betrekking tot de governance en bevindingen met betrekking tot het financieringsmodel. Daarna hebben wij enkele aandachtspunten geformuleerd met betrekking tot de business case en PSA.

Governance

Voldoen aan wet- en regelgeving

In het document is beschreven dat de systeemeigenaar toe ziet op en verantwoordelijkheid draagt voor het voldoen aan de voor de gezamenlijke biometrievoorziening relevante wet- en regelgeving (p. 30). De systeemeigenaar, pSG, tekent hiervoor als enige de SLA voor beheer namens de opdrachtgever (p.32).
De opdrachtgevers en alle onderdelen die van de service gebruik maken hebben hierin ook nadrukkelijk een eigen verantwoordelijkheid. De nieuwe privacy wetgeving laat zien dat aan het niet naleven van wet- en regelgeving straks serieuze consequenties kunnen zitten ook voor de betrokkenen zelf. Het is daarom van belang dat de verantwoordelijkheden en aansprakelijkheden binnen de keten geformaliseerd worden. Wij missen in het document daarom het afsluiten van een of meer samenwerkingsovereenkomsten (waarin tenminste is opgenomen het overeengekomen betrouwbaarheidsniveau, het stelsel van maatregelen, de controle op deze maatregelen en het toezicht daarop) en het afsluiten van weerbare bewerkersovereenkomsten met organisaties buiten VenJ.

In hoofdstuk 4 wordt beschreven waar de governance zich op richt (p. 21). In de beschreven doelstelling mist wat ons betreft de expliciete vermelding van het voldoen aan wet- en regelgeving. In de laatste versie is de doelstelling op dit punt aangepast.

Rol Beveiligingsfunctionaris en Functionaris gegevensbescherming

Wij zien in de beschrijving van de governance geen expliciete verwijzing naar de rol van de beveiligingsfunctionaris (BVA) en functionaris gegevensbescherming (FG). Gegeven het feit dat het hier biometrische gegevens betreft en dit door het CBP als bijzondere informatie (risico-klasse 3) wordt aangemerkt is het van belang deze rol voor tenminste de gezamenlijke delen nadrukkelijk te benoemen in de nadere uitwerking van de governance.

Het uitvoeren van een gezamenlijke risicoanalyse
Het gezamenlijk uitvoeren van een risicoanalyse om inzicht te krijgen in de benodigde beveiligingsmaatregelen is een activiteit die niet beschreven is in het document. De systeemeigenaar, proceseigenaren, de gegevenseigenaren dienen deze gezamenlijk uit te voeren. Deze risicoanalyse zal ook periodiek herijkt moeten worden. In ieder geval na een wezenlijke verandering van de functionaliteit. De uit de risicoanalyse voortvloeiende beheersmaatregelen dienen te worden meegenomen als eis aan de beheerpartij(en). De beheerpartij(en) dienen periodiek verantwoording af te leggen over de werking van deze maatregelen.

Eisen aan beheerpartijen
Op welke wijze toezicht wordt gehouden op de beheerpartij is nog niet nader uitgewerkt. Hiervoor kunnen ondermeer eisen worden opgenomen als 'right to audit' en/of de eis voor het jaarlijks ontvangen van een ISAE3402 verklaring.

Rol verdeling vraag- en aanbodzijde
In 4.3 en 5.3 wordt omschreven dat het (functioneel) beheer processen uitvoert "*.... voor het inventariseren, onderhouden en gericht houden van de functionele eisen en wensen van de gebruikers.*"
Dit proces behoort bij de vraagzijde in plaats van de aanbodzijde en derhalve beter gepositioneerd kan worden bij bijvoorbeeld het gebruikersoverleg. De beschrijving van de governance is op dit punt ondertussen aangepast.

Op pagina 34 is beschreven dat de beheerorganisatie gaat over het product lifecycle management. Dit kunnen wij volgen voor wat betreft bijvoorbeeld de hardwarecomponenten. Vervangingsbeslissingen in de keten (dus voor het gehele systeem) behoren echter op strategisch niveau genomen te worden genomen. Beslissingen over de functionaliteit meer op het tactisch niveau. Het lifecyclemanagement dient op strategisch en tactisch niveau te worden verduidelijkt.

Harmoniseren van processen
Het document beschrijft dat de verschillende partijen hun eigen procesinrichting kunnen blijven bepalen (p. 23 'primaire processen mogen niet in gevaar komen door het doen van compromissen'). Ook in projectbrief lezen wij dat het optimaliseren en uniformeren van de processen niet mede het doel is van het project. Afgevraagd moet worden of ook voor dit project niet eerst de processen verder geharmoniseerd moeten worden. Wij verwijzen hier naar BIT-regel 4 van de Commissie Elias die beschrijft dat eerst de processen dienen te worden gereorganiseerd en gestandaardiseerd alvorens dient te wordt gestart met het automatiseren ervan. Harmonisatie bevordert in zijn algemeenheid de implementatie (inclusief een veilige manier van werken) en levert als alle partijen het belang hiervan inzien veelal ook een verhoogde kwaliteit en efficiency.

Draagvlak
In het document is beschreven dat de oorspronkelijke aanpak gericht was op het verkrijgen van maximaal draagvlak voor het advies, maar dat dit op verzoek van het adviesteam is losgelaten (p. 7). De reden hiervoor is dat het projectteam er nog niet in is geslaagd om alle partijen voor wat betreft de governance op een lijn te krijgen. Ook hier wijzen wij op het advies van de Commissie Elias (BIT-regel 3) dat beschrijft dat draagvlak een essentiële voorwaarde is voor het slagen van het traject.

Overige opmerkingen
- In hoofdstuk 4.5. wordt op pagina 27 beschreven dat de KPI's zouden worden opgenomen in het Project Start Architectuur (PSA) document. Deze KPI's hebben wij daarin echter niet aangetroffen. Deze zijn essentieel om inzicht te krijgen in de kostenverdeling en als te stellen eisen richting leveranciers. Naar we hebben begrepen worden om praktische redenen de KPI's nu opgenomen in het programma van eisen. De beschrijving van de governance is op dit punt aangepast.
- Op operationeel niveau is invulling geven aan overleg met alle ketenpartners (dus ook buiten VenJ). Op tactisch niveau lijkt een dergelijk overleg niet voorzien. In nieuwste versie van de governance wordt dit overleg gekoppeld aan het tactische niveau. Hetgeen meer voor de hand ligt.

<u>Financieringsmodel</u>

De keuze van de verdeelsleutel
In het document is het voorstel gedaan om een verdeelsleutel te kiezen op basis van historische gegevens (hoofdstuk 6). Een dergelijk sleutel is wellicht houdbaar tot dat het systeem geïmplementeerd is. Na implementatie zal echter gekomen moeten worden tot een wijze van verrekenen die ook rekening houdt met toekomstige wijzigingen in het gebruik en transparant is voor alle partijen. Het nieuw te ontwerpen systeem biedt echter nieuwe functionaliteiten die naar verwachting ook steeds meer gebruikt zullen gaan worden en dus mogelijk ook additionele kosten met zich mee gaan brengen. Naar de echte 'kostendrivers' voor de biometrievoorziening is verder onderzoek nodig. De daadwerkelijke 'kostendrivers' zullen daarom gedurende het project in beeld moeten worden gebracht. Wij zien daarom in beginsel weinig toegevoegde waarde in het verder doorlichten van de van de huidige kosten voor het bepalen van de toekomstige verdeelsystematiek. Dit laat onverlet dat dit voor het aanscherpen van de businesscase mogelijk nog noodzakelijk is.

Overigens merken wij op dat, anders dan het financieringsmodel stelt, een complexer model voor het verdelen van de kosten niet noodzakelijkerwijs leidt tot meer tijd om te komen tot de noodzakelijke berekeningen. Afhankelijk van de kostendrivers kan het verzamelen van de benodigde gegevens en bepalen van het aandeel in het gebruik ook geautomatiseerd gebeuren.

Frictiekosten en investeringskosten
In hoofdstuk 6 wordt aangegeven dat investeringskosten transitiekosten zijn en dat ze om die redenen niet hoeven worden meegenomen bij het

kostenverdeelvraagstuk. Dit is wat ons betreft niet juist, ook aan deze kosten zit een verdeelvraag vast. Voorts zijn deze kosten naar het lijkt niet meegenomen in de businesscase. Wij zijn van mening dat deze kosten bij een zakelijke vergelijking van de kosten en de baten niet mogen ontbreken. Zij dienen dus ook in de businesscase te worden meegenomen. Het is van belang om zo snel mogelijk zicht te krijgen op de omvang van deze frictiekosten. Hetgeen niet eenvoudig is vanwege de onduidelijkheid over het moment van aansluiten door de diverse partijen.

Onderdeel van de frictiekosten bij de enkelvoudige beheervariant zijn mogelijk ook de vervroegde afschrijving van hard- en software en de kosten in verband personele aanpassingen bij de huidige beheerders.
Een belangrijk aandachtspunt is dat de frictiekosten dienen te worden voorgefinancieerd. Hierbij geldt dat dit bij een batenlastendienst niet via de leenfaciliteit van het ministerie van Financiën kan. Voor deze kosten zal daarom ruimte in de in de begroting gevonden moeten worden.

Aandachtspunten Business case en PSA
Hoewel de Business case en de PSA feitelijk buiten de scope van ons onderzoeken vallen, hebben wij gemeend daarover toch enkele aandachtspunten te moeten formuleren. Over de business case merken wij het volgende op:
- Uit de stukken komt niet naar voren waarom een ABIS voor alle partijen een meerwaarde biedt boven een AFIS. De keuze voor een ABIS wordt als uitgangspunt gehanteerd.
- De financiële business case houdt geen rekening met een ander gebruik van de ABIS dan voor de vingerafdruk. Ten tijde van het opstellen van de business case lijkt nog onvoldoende zicht te zijn om de (on)mogelijkheden van een ABIS en de gebruiksmogelijkheden hiervan voor de praktijk. Het actualiseren van de business case na de marktverkenning lijkt daarom noodzakelijk.
- De huidige business case houdt geen rekening met de keuzes die er zijn voor het moment van aansluiten en de wijze van beheren (enkelvoudig ten opzichte van meervoudig beheer). De reden hiervoor is dat de frictiekosten buiten beschouwing zijn gelaten.
- Het aansluiten van de Nationale politie (voor vervanging HAVANK) lijkt van belang voor een positieve businesscase. Rondom deze aansluiting bestaat momenteel nog de meeste onzekerheid, in ieder geval lijkt de Nationale politie als laatste aan te sluiten met hoge frictiekosten tot gevolg.
- De veronderstelling dat een gezamenlijk traject leidt tot scherpere aanbiedingen vanuit de markt (p. 33) is niet onderbouwd. Een gezamenlijk traject is immers groter en complexer dan een aantal afzonderlijke trajecten. Mogelijk kan slechts een beperkt aantal leveranciers een dergelijk complex traject aan, wat juist kostenopdrijvend kan werken.

Volgens best practise maken de beveiligingseisen (security) onderdeel uit van de feasability fase. Deze fase behoort voor de business case afgerond te zijn. In de PSA valt ons op dat het aspect security heel beperkt aan de orde komt, terwijl dit een essentieel onderwerp is gegeven het karakter van het systeem. Het projectteam heeft naar wij hebben begrepen besloten om dit aspect in een separaat traject op te pakken.

Auditdienst Rijk
Clustermanager Veiligheid en Justitie

J.P. Looman RA CIA

Auditdienst Rijk

Ons kenmerk
ADR/ 2015/963